



Beyond troubleshooting

A mission-first help desk model

Table of contents

Executive summary	03
The challenge: Bridging the support-security paradox	04
The solution: High-assurance managed services	04
The four pillars of technical integrity	05
Strategic governance and program management.....	06
Case study: Rapid P1 escalation and multi-vendor forensic analysis... 	08
Operational excellence management	10
The agile support framework	12
Case study: Resilience through proactive service excellence.....	13
Three high-assurance support tiers.....	15
Proven performance and mission impact	17
The strategic advantage for mission-ready operations.....	19

Executive summary

In the high-stakes environment of U.S. government operations, technical support is a cornerstone of national security and operational readiness. TTEC Government Solutions provides a specialized Public Service Center (PSC) engineered specifically for the unique mission requirements of defense and federal agencies. Staffed exclusively by U.S. citizens operating remotely within the United States, our support model ensures that mission-critical platforms remain secure, optimized, and available 24/7/365. By combining a 15-minute response target for critical incidents with a robust zero trust architecture, TTEC Government Solutions sets the gold standard for secure government managed services.

The challenge

Bridging the support-security paradox

Government agencies often struggle to find a balance between rapid technical resolution and rigorous security compliance.

Reactive delays:

Traditional help desks often wait for total failure before acting, leading to significant mission downtime.

Compliance risks:

Generic providers may utilize non-cleared personnel or insecure authentication methods that do not meet CMMC L2 standards.

Operational friction:

A lack of specialized change management can lead to unauthorized modifications or system instability.

The solution

High-assurance managed services

TTEC Government Solutions bridges the gap by integrating engineering-level expertise directly into the support workflow.

Hardened infrastructure:

Our ServiceNow platform is engineered to FedRAMP High specifications, supported by a methodology and expert personnel capable of scaling to meet the most demanding national security requirements. TTEC Government Solutions currently adheres to CMMC Level 2 standards, ensuring the secure processing and protection of controlled unclassified information (CUI).

U.S.-based personnel:

All support services are delivered exclusively by U.S.-based resources, ensuring full compliance with stringent federal residency and citizenship requirements. At a minimum, every member of our support team is required to possess and maintain a Public Trust clearance, ensuring a vetted and reliable workforce for every interaction.

Round-the-clock vigilance:

We provide continuous 24/7/365 coverage for critical and high-severity incidents.

The four pillars of technical integrity

Our ITIL-based change enablement framework ensures that every modification — from routine MACDs to urgent fixes — is authorized, documented, and risk-mitigated to maintain the integrity of mission-critical systems.

System & service change categories

Category	Description	Examples
 MACD changes	Moves, adds, changes, and deletes to facilitate user and software configuration.	Adding users, configuring phones, or adding new lines.
 Platform management	Proactive maintenance and health monitoring of the system.	OS and vulnerability patching, server health monitoring, and security operations.
 Project changes	Modifications driven by post-production project requirements.	Adding new features outside of standard support.
 Incident related	Changes created specifically as a solution to identified outages.	Urgent fixes derived from Level 1 incident evidence.

The ITIL advantage: Disciplined, responsive, secure

Adhering to global service management standards allows us to minimize risk, ensure CMMC L2 and FedRAMP High regulatory alignment, and increase operational velocity through pre-authorized standard changes. Our disciplined approach delivers:



15-minute P1 and P2 response by U.S.-based engineers



Forensic root cause analysis (RCA) delivered within 5-7 business days



Disciplined RFC process across all MACD and platform updates



Automated monthly reporting via our FedRAMP High ServiceNow portal

Strategic governance and program management

TTEC Government Solutions offers a disciplined management structure that integrates security compliance and project rigor throughout the entire lifecycle of our partnership. Our leadership is committed to the success of your mission, from initial project delivery through the years of sustained support that follow.

Project management office: Continuous lifecycle accountability

Our government project management office (PMO) maintains ultimate responsibility for the integrity of the contract throughout its duration. To provide a high-assurance interface, we utilize a single point of contact (SPOC) model, creating a persistent bridge of accountability between your agency and our technical teams.



Key benefits

Unified security oversight:

The government PMO oversees end-to-end mission security. Every interaction is vetted against federal safeguarding protocols and the program's specific residency and security requirements.

Continuous lifecycle management:

By maintaining the same PMO oversight from project handoff through long-term support, we eliminate the "knowledge gaps" common in traditional vendor transitions.

Streamlined accountability:

Your agency has one clear path for communication, backed by leadership with the authority to ensure technical performance and security compliance.

Technical manager: Engineering meets mission strategy

A cornerstone of our disciplined approach is the technical manager, who serves as the primary technical leader and customer liaison. The technical manager bridges the gap between complex backend engineering and your agency's operational needs.

Working in lockstep with our Level 2 and Level 3 engineers and the PMO, the technical manager translates deep technical data into clear, mission-focused explanations. When a system modification is proposed, the technical manager interfaces directly with the customer to:

Explain technical changes: Providing clarity on the technical “how” and “why” behind every update.

Seek authorization: Ensuring all changes are fully understood and formally approved by agency stakeholders before implementation.

Ensure technical integrity: Coordinating with senior engineers to guarantee that every solution is technically sound and aligned with mission goals.

In a mission-critical environment, technical support frequently uncovers the need for system enhancements or modernization. Our model ensures these transitions are handled with the same rigor as the initial project start.

Key benefits

Ensured technical continuity:

All project work identified during the support phase is initially managed by our technical manager, preventing the loss of critical mission context during the transition from a support ticket to a system enhancement.

Synchronized strategic execution:

For larger initiatives, our PMP-certified project managers and technical managers work in tandem. This dual-layer leadership ensures the deep technical expertise of our senior engineers is perfectly synchronized with the agency's strategic project goals and timelines.

Authorized transparency:

Our technical managers act as the primary interface for your stakeholders, translating complex backend data into clear, mission-focused explanations. This ensures every system change is fully understood, authorized, and documented, maintaining the agency's total control over the platform's evolution.

Rapid P1 escalation and multi-vendor forensic

The challenge

During a high-tempo operational period, agents at a U.S. military service desk began experiencing a critical system failure where CRM sessions would disconnect immediately after a call ended. While active calls remained stable, the logout forced agents to manually re-authenticate after every interaction, severely impacting the program's ability to maintain "at the ready".

Our approach

This incident demonstrated the value of our flexible engagement model and the importance of customer-driven priority control.

- **16:13:** An initial inquiry was opened via the ServiceNow portal as a low-priority ticket while the agency assessed the scope.
- **17:55:** Recognizing the disruption was broader than initially thought, the client utilized our single-number hotline to initiate the "Phone-First" escalation protocol.
- **17:56:** In accordance with our 15-minute P1 response protocol, a Tier 2 engineer took the case immediately and restored service by 18:50.

The forensic deep dive

Our model focuses on more than just the immediate fix; we prioritize long-term stability through forensic accountability.

Proactive probing: Although the issue appeared cleared, the Tier 2 engineer probed further and opened a case with the hardware vendor to review logs.

SME integration: The vendor identified a carrier equipment hit in Denver, Colorado. A Tier 3 SME immediately took the case to correlate these findings with internal status logs, confirming a private network outage as the root cause.

Mission alignment: The technical manager served as the "technical bridge," maintaining persistent communication with the U.S. military stakeholders to explain the multi-vendor dependency of the failure.



The resolution

Despite the incident occurring during a holiday week, TTEC Government Solutions maintained its commitment to rigorous documentation.

Root cause identified: The investigation proved that carrier-level circuit bounces caused both processors to enter a disconnect status, triggering the agent logouts.

Timely delivery: The technical manager delivered the formal root cause analysis (RCA) to the client on 12/28, meeting our 5–7 business day commitment even during a federal holiday period.

Key benefits

Empowered decision-making:

The client remained in control of the mission's path, using the phone escalation to move the help desk from a low response to an immediate P1 engineering focus.

Forensic depth: By involving Tier 3 SMEs and hardware vendors, we identified an external carrier hit that a standard help desk would likely have missed as a transient issue.

Lifecycle stewardship: The government PMO and technical manager ensured that even with a multi-vendor root cause, the agency had a single path for accountability and a permanent record for problem management follow-up.

Operational excellence management

Serving as the strategic alignment lead, the executive director acts as the critical bridge between the government PMO and the service desk, providing the tactical governance necessary to maintain a world-class Public Service Center (PSC). This leadership layer is responsible for the overall health of the service desk, ensuring that every support engineer is not only technically proficient but also mission-aligned and consistently synchronized with the agency's mission and security standards.

Under the executive director, the service desk management team leads the engineers in four critical areas of operational discipline:

Security alignment: They ensure that every support engineer strictly adheres to the security requirements set by security oversight. This includes maintaining residency compliance and following the zero trust journey for every system of access.

ITIL practice adherence: Management ensures that ITIL standards for incident, change, and problem management are woven into the team's daily workflow, providing the auditable trail required for government oversight.

Customer-defined priorities: They enforce the mission-first mindset, ensuring engineers prioritize incidents based on the agency's definition of mission impact, not just internal metrics.

Knowledge base (KB) maturity: Leadership oversees the development of a robust, technical knowledge base. This ensures that support engineers have the forensic data they need at their fingertips to resolve complex issues rapidly.

Information integrity via secure knowledge base

A vital component of service desk management is protecting the "brain" of the operation — the ServiceNow knowledge base. In our support model, information is a protected asset. The executive director and the management team ensure that:

Matured information: The knowledge base is constantly updated and "matured" with forensic data from root cause analyses (RCAs) and project handoffs, ensuring engineers aren't starting from scratch.

Protected access: All technical documentation, sensitive configurations, and mission-specific data within ServiceNow are protected. Access is strictly governed by the same zero trust and identity verification protocols that protect the platform itself.

Data safeguarding: Information is tiered and tagged within ServiceNow to ensure it is handled according to its specific federal safeguarding requirements, preventing data leakage and ensuring compliance with CMMC L2 standards.

Continuous improvement via annual surveys

While real-time metrics provide a snapshot of performance, TTEC Government Solutions utilizes formal annual customer satisfaction (CSAT) surveys to capture the long-term health of our partnership. This structured feedback loop is a vital component of our continual service improvement (CSI) strategy, allowing us to:

Audit technical competency: We measure user confidence in our engineers' ability to resolve complex, high-stakes incidents with precision.

Evaluate communication clarity: Surveys assess the effectiveness of our technical managers and Tier 3 engineers in translating engineering data into actionable mission intelligence.

Drive strategic alignment: Feedback is reviewed by the executive director and shared with the PMO to ensure our service roadmap evolves alongside the agency's mission.



Performance transparency via monthly reporting

To ensure total mission transparency, TTEC Government Solutions provides comprehensive automated monthly reporting. We move beyond static spreadsheets by providing stakeholders with direct, real-time access to call metrics and incident data via our ServiceNow portal. Our reporting model is designed for maximum flexibility, allowing the technical manager to tailor the delivery to the agency's specific needs:

Consultative setup: The technical manager collaborates with the mission customer to define critical success factors and configure automated dashboards that reflect the metrics most important to their operation.

Strategic cadence: For complex missions, the technical manager personally runs and analyzes these reports to facilitate regular cadence meetings, providing context and forensic insight into performance trends.

Direct delivery: If the client prefers a hands-off approach, the technical manager can configure ServiceNow to automatically deliver standardized reports directly to the agency's leadership, ensuring consistent visibility with zero administrative burden.

The agile support framework

Our Public Service Center (PSC) integrates the PMO directly into the service desk flow, ensuring every inquiry reaches the right expertise with maximum velocity and zero bureaucratic delay.

1. Precision intake and triage

Every inquiry begins with a **ServiceNow (SNOW)** ticket, our system of record for all technical activity. This digital-first approach ensures every interaction is captured, timestamped, and categorized to maintain alignment with federal safeguarding requirements and ITIL best practices.

2. Rapid resolution with CRB (minor changes)

For requests requiring under 10 hours of work, our model is built for speed.

Nimble governance: A daily government PMO change review board (CRB) reviews, authorizes, and implements minor changes in near real-time.

Engineer-led execution: Support engineers document the change, secure customer approval via the ticket, and apply the fix to keep your platform optimized without the wait.

3. Scaled project rigor (major changes)

If a request exceeds 10 hours, our Tier 1 and Tier 2 engineers collaborate with the PMO to assess the level of effort and the best mission-aligned response.

Iterative requirements: The PMO works with you to define exact requirements and provide a formal quote.

Collaborative delivery: Once funded, project and support engineers plan and deploy the new capability.

Full-circle support: New work is integrated back into the support model with matured knowledge base articles for Day 1 readiness.

Key benefits

Velocity: Small changes happen daily, not weekly.

Transparency: Customers approve all actions via the ServiceNow portal.

Accountability: PMO and operations leadership oversee both tickets and projects to prevent information loss.

Resilience through proactive service excellence

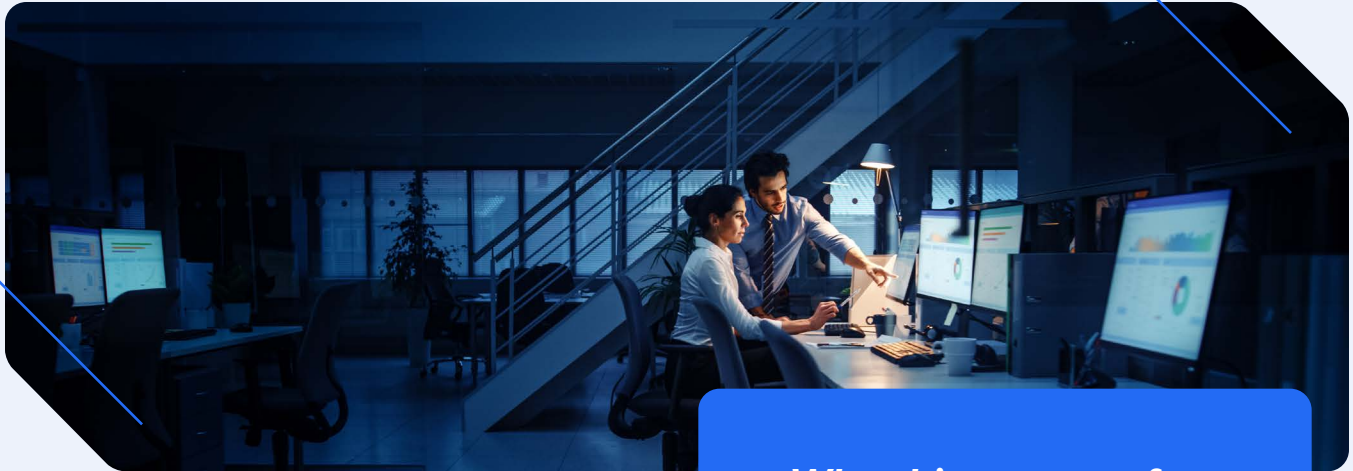
The challenge

Following scheduled power maintenance at a U.S. military installation, a critical WAN router suffered a catastrophic hardware failure. The location was “down hard,” severing VPN connectivity for the site.

Our approach

While traditional help desks wait for a user to report a blackout, our integrated monitoring tools identified the issue before the start of the standard business day.

- **06:58:** Automated monitoring detected the device failure and instantly opened a ServiceNow ticket.
- **07:18:** Proactive monitoring flagged the event for human review within 20 minutes.
- **07:26:** Within 8 minutes of review, a TTEC Engineer confirmed the site was down and escalated the ticket to Priority 1 (P1).
- **07:36:** The technical manager was notified and immediately began coordinating between the military stakeholders, the carrier, and the hardware vendor.
- By **08:44**, the technical manager performed a mission-impact assessment. Recognizing that agents remained operational via mobile applications and that the failure was isolated to a single site, the technical manager collaborated with the client to downgrade the incident to Priority 2 (P2). This strategic move allowed the team to focus on the complex, multi-day RMA logistics without triggering unnecessary emergency protocols.



The resolution

TTEC Government Solutions managed the complex recovery lifecycle, including navigating vendor contract hurdles and coordinating onsite technicians.

RMA management: An RMA was initiated by 08:52 on Day 1.

Technical integrity: TTEC Government Solutions engineers worked through OS configuration issues and connectivity hurdles to restore full operational status.

Forensic reporting: Following restoration, our team produced a detailed RCA to identify the hardware root cause and recommend cold spare strategies for future site hardening.

Why this matters for the mission owners

Velocity: Detection occurred before the business day began, allowing for an RMA to be initiated within hours of failure.

Transparency: The technical manager provided a persistent bridge of communication between the U.S. military, the carrier, and the vendor.

Matured knowledge: The findings from this RCA were matured into our knowledge base to optimize response times for similar power-maintenance events across the enterprise.

Three high-assurance support tiers

TTEC Government Solutions utilizes a tiered engineering model designed to provide immediate technical resolution while ensuring long-term platform stability. Every tier is staffed by U.S. citizens and operates 24/7/365 to support your mission-critical SaaS environment.



Tier 1: Engineering

Focus

Proactive/reactive intake

Availability

24/7/365

Citizenship

100% U.S. citizen

Response

Instant / 15-min P1 & P2



Tier 2: Service delivery

Focus

Escalated resolution

Availability

24/7/365

Citizenship

100% U.S. citizen

Response

Immediate escalation



Tier 3: (SME) Subject matter expert

Focus

RCA & platform hardening

Availability

Business hours + on-call

Citizenship

100% U.S. citizen

Response

Deep forensics analysis

Tier 1: Engineering-led frontline support

Unlike traditional help desks that rely on non-technical dispatchers, our Tier 1 is comprised of engineer resources.

Proactive system vigilance:

Our Tier 1 team performs continuous proactive monitoring to identify and remediate potential system anomalies before they impact mission operations.

Rapid incident management:

Responsible for the initial triage and resolution of reactive incidents, ensuring that critical issues are addressed immediately upon detection.

Operational intake:

Manages the initial secure intake and verification of all service requests, maintaining a disciplined entry point for the support lifecycle.

Tier 2: Advanced service delivery

When a request requires deeper analysis or specialized configuration, it is escalated to our service delivery specialists.

Complex problem diagnosis:

Handles escalated incidents involving critical system components, quality concerns, and multi-user service degradations.

Change lifecycle oversight:

Manages the technical execution of platform modifications, ensuring all changes are aligned with the program's lifecycle requirements.

Mission continuity:

Focuses on ensuring that the platform remains optimized for the client's specific operational flows and program objectives.

Tier 3: Specialized subject matter experts (SME)

Tier 3 serves as the highest level of technical authority, providing the deep forensic and architectural oversight necessary for complex government infrastructures.

Forensic root cause analysis (RCA): Our Tier 3 engineers lead the forensic investigation into any P1 incident. We deliver a comprehensive, formal RCA to the client within 5-7 business days of service restoration, detailing exactly what occurred and the measures taken to prevent recurrence.

Strategic platform evolution: Responsible for large-scale project changes and high-level infrastructure enhancements. This team ensures that as the agency's mission grows, the underlying platform architecture evolves to maintain peak performance and security.

Advanced remediation: Provides the final word on the most complex technical challenges that require deep subject matter expertise in IL4 environment configurations and SaaS interoperability.

Architectural hardening: Continuously evaluates the platform's security posture and health, implementing the advanced engineering controls required to maintain its FedRAMP High and CMMC L2 standing.

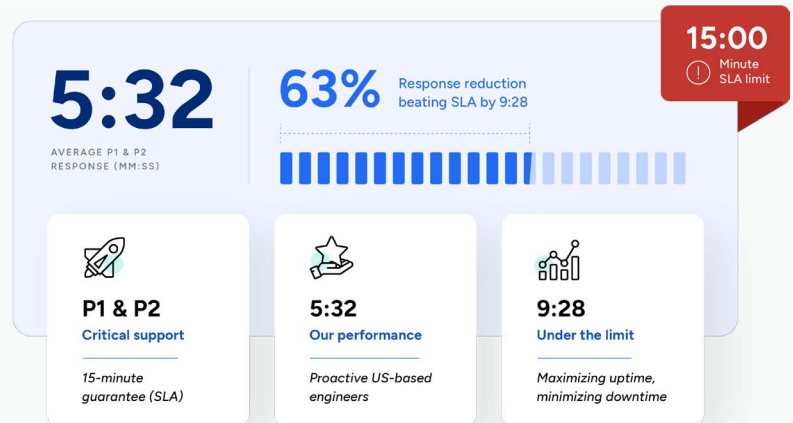
Proven performance and mission impact

SLA achievement

TTEC Government Solutions offers a 15-minute response guarantee with an actual average of 5:32 — all while maintaining 100% compliance with NIST, CMMC, and NISPOM standards. Our U.S.-based, cleared engineers ensure that your most sensitive workloads are both responsive and resilient.

SLA achievement: P1 & P2 response time

We don't just meet expectations — we beat them!



* Based on critical incident (P1 & P2) in the selected period

Accelerated restoration

Our 1:50:06 controllable mean time to restore (cMTTR) is a direct result of our daily CRB model and the proactive coordination of our technical managers, ensuring that every second of active time is focused exclusively on mission restoration. By focusing on controllable time, we provide a forensic view of our Tier 1, 2, and 3 engineering velocity. It proves that when a mission is in our hands, the path to resolution is measured in minutes and hours, not days. This transparency allows your agency to see exactly how our agile support framework eliminates internal bureaucratic lag while we simultaneously manage the complexities of your external vendor environment.

Compliance badges

Our performance is anchored by a security-first architecture. Every action taken during our 5:32 average response is governed by strict adherence to the most rigorous federal compliance frameworks, ensuring that speed never compromises the integrity of your most secure environments.

NIST 800-171/172: Delivering the foundation for protecting CUI across all service platforms.

Cybersecurity Maturity Model Certification (CMMC): Ensuring institutionalized cybersecurity readiness for DoW contract requirements.

National Industrial Security Program (NISPOM): Strict adherence to FSO-led protocols for handling classified and sensitive information.

FedRAMP High/IL4-IL5: Maintaining secure enclaves and CSP environments specifically engineered for government data sovereignty.

Streamlined support for high-stakes operations

TTEC Government Solutions provides a unified support ecosystem designed to eliminate bureaucratic silos. Because clear communication is paramount during service degradations, we offer flexible, high-velocity engagement methods that meet your users exactly where they are — ensuring no time is lost in a high-stakes environment.

To ensure maximum availability, our Public Service Center (PSC) is accessible via two primary channels, both operating 24/7/365:

- 1. **Single-number hotline (preferred for P1/P2):** For urgent, mission-impacting issues, we maintain a single, dedicated phone line. This provides immediate access to a live U.S.-based support engineer. For P1 and P2 incidents, we encourage a phone approach to trigger our 15-minute response protocol instantly.
- 2. **ServiceNow (SNOW) portal:** For standard requests (P3/P4) or to provide detailed technical data, logs, and screenshots, users can utilize our secure, FedRAMP High portal. This provides a transparent, auditable trail of the request from intake to resolution.

Our support model is designed to be as nimble as the mission requires. We empower users to define their level of urgency through a collaborative intake process:

Direct intake: You call us, and we open the ticket for you, capturing the details in real-time.

Detail intake: You open a ticket in the SNOW portal with all necessary technical details.

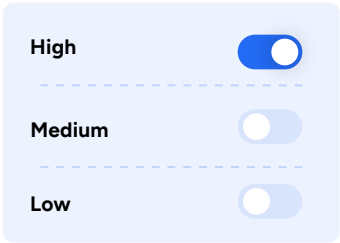
The priority trigger: Once a ticket is in the system, a quick follow-up call allows the user to immediately escalate that ticket to the required priority level. This ensures your mission — not the help desk — remains in control of the impact designation.

Ultimate control: You determine the mission's path

Empowered decision-making at every step. Your judgment is paramount.

You determine the priority

Set the order. Define the urgency. Your decision drives the workflow.



You remain in control of the mission's path

Access the consequence. Designate the severity. You define the mission's stakes.



The strategic advantage for mission-ready operations

TTEC Government Solutions provides far more than a standard help desk; we deliver a distinct strategic advantage. Our true strength lies in our people — U.S.-based experts who possess a deep, innate understanding of the complexities of government operations and national security. By combining this human capital with a battle-tested methodology, we empower your agency to remain focused on its core mission while we ensure your communication platform is secure, optimized, and mission-ready in any environment.

Ready to secure your mission?

Contact: Aaron Mosby

Email: aaron.mosby@ttecdigital.com

Phone: 202-459-3075



Aaron Mosby

Vice President, Digital
Sales - Public Sector

About TTEC Government Solutions

TTEC Government Solutions, a subsidiary of TTEC Holdings, Inc. (NASDAQ: TTEC), is a premier provider of AI-enabled digital customer experience (CX) technology and services for federal, state, and local government agencies. Leveraging a 40-year history of CX excellence, TTEC integrates FedRAMP-authorized cloud contact center solutions (CCaaS), omnichannel engagement platforms, and advanced analytics to modernize citizen services, increase operational efficiency, and deliver seamless, secure interactions.